CLAIMS

What is Claimed is:

1. A method of storing program material for subsequent replay, comprising the steps of:

(a) accepting encrypted access control information and the program material encrypted according to a first encryption key, the access control information including a first encryption key and control data;

(b) decrypting the received access control information to produce the first encryption key;

(c) decrypting the program material using the first encryption key;

(d) re-encrypting the program material according to a second encryption key;

(e) encrypting the second encryption key according to a third encryption key to produce a fourth encryption key; and

(f) providing the re-encrypted program material and the fourth encryption key for storage.

2. The method of claim 1, wherein the encrypted access control information further comprises temporally-variant control data, and the method further comprises the steps of:

decrypting the received access control information to produce the temporally-variant control data; and

modifying the temporally variant control data to generate temporally-invariant control data.

3. The method of claim 1, wherein steps (b) and (e) are performed in a conditional access module.

4. The method of claim 3, wherein the conditional access module is implemented on a smartcard communicatively coupleable to a tuner and a media storage device.

5. The method of claim 1, wherein the access control information further comprises metadata describing at least one right for the program material.

6. The method of claim 5, further comprising the step of:
generating the second encryption key at least in part from the metadata.

7. The method of claim 1, wherein steps (b)-(f) are performed in response to a pre-buy message.

8. The method of claim 7, wherein the access control information further comprises metadata describing at least one right for the program material, and the method further comprises the step of:
generating replay right data from the metadata.

9. The method of claim 8, wherein the replay right data is further generated from pre-buy data.

10. The method of claim 1, further comprising the steps of:
retrieving the stored re-encrypted program material and the fourth encryption key;
decrypting the fourth encryption key using the third encryption key to produce the second encryption key; and
decrypting the re-encrypted material using the second encryption key.

11. The method of claim 10, wherein the step of decrypting the fourth encryption key using the third encryption key to produce the second encryption key is performed in response to a subscriber request to access the program material.

12. The method of claim 11, wherein the access control information further comprises metadata describing at least one right for the program material, the subscriber request to access the program material comprises buy data, and the method further comprises the steps of:

generating replay right data from the metadata;

accepting the buy data;

comparing the buy data with the replay right data; and

decrypting the fourth encryption key using the third encryption key to produce the second encryption key according to the comparison between the buy data and the replay right data.

13. The method of claim 12, wherein steps (b)-(f) are performed in response to a pre-buy message, and wherein:

the second encryption key and the third encryption key are stored in a smartcard, and the replay right data is generated from the metadata and the pre-buy message in the smartcard; and

the steps of accepting the buy data, comparing the buy data with the replay right data, and decrypting the fourth encryption key using the third encryption key to produce the second encryption key according to the comparison between the buy data and the replay right data are performed in the smartcard.

14. The method of claim 1, wherein the re-encrypted program material and the fourth encryption key are stored on a media storage device.

15. The method of claim 1, wherein the control data is temporally-variant.

16. The method of claim 15, wherein the temporally-variant control data associates an expiration time with the program material.

17. An apparatus for storing program material encrypted according to a first encryption key for replay, comprising:

a conditional access module, for accepting encrypted access control information including the first encryption key and temporally-variant control data, the control access module comprising:

a first decryption module, for decrypting the access control information to produce the first encryption key;

a first encryption module, for encrypting a second encryption key with a third encryption key to produce a fourth encryption key; and

a second decryption module for decrypting the fourth encryption key to produce the second encryption key.

18. The apparatus of claim 17, further comprising:

a tuner, communicatively coupleable to the conditional access module for receiving the encrypted access control information and the program material encrypted according to a first encryption key;

a third decryption module, for decrypting the program material using the first encryption key produced by the conditional access module;

a second encryption module, for re-encrypting the decrypted program material according to the second encryption key; and

a fourth decryption module, for decrypting the re-encrypted program material according to the second encryption key.

19. The apparatus of claim 18, wherein the conditional access module further comprises:

a pre-buy module, for controlling the first decryption module.

20. The apparatus of claim 18, wherein the access control information further comprises metadata describing at least one right for the program material.

21. The apparatus of claim 20, wherein pre-buy module generates replay right data from the metadata.

22. The apparatus of claim 21, further comprising a buy module, communicatively coupled to the pre-buy module.

23. The apparatus of claim 22, wherein the buy module comprises:

a purchase module for accepting buy data and comparing the buy data and the replay right data from the pre-buy module; and

a control module for controlling the second decryption module based on the comparison between the buy data and the replay right data.

24. The apparatus of claim 23, further comprising a billing module, for recording the buy data.

25. The apparatus of claim 18, wherein the second encryption key is stored in the conditional access module.

26. The apparatus of claim 18, wherein the third encryption key is stored in the conditional access module.

27. The apparatus of claim 17, wherein the conditional access module is releaseably communicative coupleable to:

a tuner for receiving the encrypted access control information and the program material encrypted according to a first encryption key;

a third decryption module, for decrypting the program material using the first encryption key from the conditional access module

a second encryption module, for re-encrypting the decrypted program material according to the key; and

a media storage device.

28. An apparatus for storing program material for replay, comprising:

means for accepting encrypted access control information and the program material encrypted according to a first encryption key, the access control information including a first encryption key and control data;

means for decrypting the received access control information to produce the first encryption key;

means for decrypting the program material using the first encryption key;

means for re-encrypting the program material using according to a second encryption key;

means for encrypting the second encryption key according to a third encryption key to produce a fourth encryption key; and

means for providing the re-encrypted program material and a fourth encryption key for storage.

29. The apparatus of claim 28, wherein the encrypted access control information further comprises temporally-variant control data, and the apparatus further comprises:

means for decrypting the received access control information to produce the temporally-variant control data; and

means for modifying the temporally variant control data to generate temporally-invariant control data.

30. The apparatus of claim 28, wherein the means for decrypting the received access control information to produce the first encryption key and the means for encrypting the second encryption key according to a third encryption key to produce a fourth encryption key are implemented in a conditional access module.

31. The apparatus of claim 30, wherein the conditional access module is implemented on a smartcard communicatively coupleable to a tuner and a media storage device.

32. The apparatus of claim 28, wherein the access control information further comprises metadata describing at least one right for the program material.

33. The apparatus of claim 32, further comprising:

means for generating the second encryption key at least in part from the metadata.

34. The apparatus of claim 32, further comprising:

means for generating replay right data from the metadata.

35. The apparatus of claim 34, wherein the means for generating the replay right data further generates replay right data from pre-buy data.

36. The apparatus of claim 30, further comprising:

means for retrieving the stored re-encrypted program material and the fourth encryption key;

means for decrypting the fourth encryption key using the third encryption key to produce the second encryption key; and

means for decrypting the re-encrypted material using the second encryption key.

37. The apparatus of claim 36, wherein the means for decrypting the fourth encryption key using the third encryption key to produce the second encryption key is performed in response to a subscriber request to access the program material.

38. The apparatus of claim 37, wherein the access control information further comprises metadata describing at least one right for the program material, the subscriber request to access the program material comprises buy data, and the apparatus further comprises:

means for generating replay right data from the metadata;

means for accepting the buy data;

means for comparing the buy data with the replay right data; and

means for decrypting the fourth encryption key using the third encryption key to produce the second encryption key according to the comparison between the buy data and the replay right data.

39. The apparatus of claim 38, wherein:

the second encryption key and the third encryption key are stored in a smartcard, and the replay right data is generated from the metadata and the pre-buy message in the smartcard; and

the means for accepting the buy data, means for comparing the buy data with the replay right data, and means for decrypting the fourth encryption key using the third encryption key to produce the second encryption key according to the comparison between the buy data and the replay right data is implemented in the smartcard.

40. The apparatus of claim 28, wherein the re-encrypted program material and the fourth encryption key are stored on a media storage device.

41. The apparatus of claim 28, wherein the control data is temporally-variant.

42. The apparatus of claim 41, wherein the temporally-variant control data associates an expiration time with the program material.